

REMARKS

By this amendment, claim 1 has been amended. In the Office Action, the Examiner rejected claims 1-3 under 35 U.S.C. §102(b) as being anticipated by Schneier¹ "Applied Cryptography"; and rejected claims 4-6 under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Italia et al. ("Italia") (U.S. Patent No. 6,792,111).

A. Claim Rejection - 35 U.S.C. § 102(b)

Applicant respectfully traverses the rejection of claims 1-3 as being anticipated by Schneier because Schneier fails to disclose every claim element. For example, independent claim 1 recites a combination of steps, including, *inter alia*, "carrying out said cryptographic communication of information by applying said combination of chaos block encryption and said chaos stream encryption *to the information*." Schneier fails to disclose at least these claim elements.

The Office Action describes Schneier as combining block encryption and stream encryption. See Office Action at page 2 citing Schneier, Fig. 8.17 at page 175. Schneier discloses using a stream cipher in output feedback mode, with the block algorithm acting as a next-state function. See Schneier, Fig. 8.17 at page 175). However, Schneier only discloses the stream cipher in output feedback mode as a "keystream generator". See, Schneier at page 175. Schneier does not disclose the use of the stream cipher for carrying out cryptographic communication of information.

¹ The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement or characterization in the Office Action.

Information communicated by the communication method of claim 1 is distinct from the key generated by the stream cipher disclosed by Schneier. See Schneier, Fig. 8.17 at page 175; see also amended claim 1 at page 2 of this Reply. Therefore, Schneier fails to disclose “carrying out said cryptographic communication of information by applying said combination of chaos block encryption and said chaos stream encryption *to the information*,” as claimed in claim 1.

Schneier also fails to disclose every element of independent claim 2. For example, independent claim 2 recites a combination of elements, including, *inter alia* “said plural CPUs, *after enciphering a plaintext code* which is a secrecy object by chaos block encryption, encipher by chaos stream encryption and transmit an obtained cipher code . . .”. Schneier fails to disclose at least these claim elements.

In the Office Action, the Examiner maintained that Schneier discloses enciphering a plaintext code which is a secrecy object by block encryption, encipher by stream encryption and block encryption and restore the block encryption (cipher) as the original plaintext code. See Office Action at pages 2-3 (citing Schneier at pages 176 and 177). Schneier discloses the use of a keystream generator in counter mode, with the block algorithm acting as an output function, wherein the least significant bit of the block algorithm’s output becomes the output of the keystream generator. See Schneier, Fig. 8.18 at page 176. Similarly, Schneier also discloses the use of a keystream generator in cipher-feedback mode using a block algorithm, wherein the least significant bit of the block algorithm’s output becomes the output of the keystream generator. See Schneier, Fig. 8.19 at page 176. In both these instances, the “internal state” of the keystream generator is the input to the block algorithm. See Schneier, Figs. 8.18 and

8.19 at page 176. Thus, the block algorithm in both these instances enciphers the internal state of the keystream generator. However, Schneier discloses that the internal state of the keystream generator is the “previous n ciphertext bits”. See Schneier, at pages 175-76. Enciphering ciphertext bits does not constitute “*enciphering a plaintext code* which is a secrecy object by chaos block encryption,” as included in claim 2.

Independent claim 3, although different in scope, includes elements corresponding to the elements of claim 2. Therefore, independent claim 3 is allowable for at least the reasons discussed above.

B. Claim Rejection - 35 U.S.C. § 103(a)

Claims 4-6 depend from and add additional features to independent claims 1-3. Moreover, Italia, relied on for its disclosure of respective data bases for a cipher key, a cipher table, and a restoration table (see Office Action at page 3, paragraph 9), fails to cure the deficiency of Schneier. Accordingly, claims 4-6 are allowable for at least the reasons set forth above.

C. Conclusion

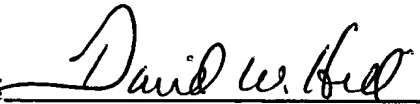
In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: August 29, 2005

By: 
David W Hill
Reg. No. 28,220